

REMARKS

In response to the Final Office Action mailed on September 19, 2005, Applicant respectfully requests reconsideration. Claims 1-4, 6-27 and 29-34 were previously pending for examination. No claims have been amended, canceled or added by this response. Accordingly, claims 1-4, 6-27 and 29-34 are pending in this application, of which claims 1, 15 and 21 are independent.

Initially, Applicant appreciates the courtesy extended by Examiner Dinh in conducting the telephone interview on November 15, 2005, the substance of the which is summarized below. During the telephone conference, Applicant's representatives argued that there was no motivation to combine Ericson and Yu. The Examiner maintained the position asserted in the Office Action and no agreement was reached.

Applicant continues to believe the claims as pending distinguish over the prior art of record, and fear that an impasse may have been reached such that an appeal may be necessary. Given that, Applicant has prepared this Response in the form of an appeal brief so that in the event this Response does not place the application in condition for allowance, Applicant can simply file the brief. However, Applicant would prefer to reach agreement without the necessity of an appeal, and invites the Examiner to contact the undersigned if, after reviewing this Response, that appears to be possible.

I. REAL PARTY IN INTEREST (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in this application is the assignee, EMC Corporation, a Massachusetts corporation having a place of business at 171 South Street, Hopkinton, Massachusetts 01748.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. §41.37(c)(1)(ii))

There are no other appeals or interferences known to the Applicant, the Applicant's legal representative, or the assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in an appeal.

III. STATUS OF CLAIMS (37 C.F.R. §41.37(c)(1)(iii))

There are 32 total claims in this application (3 independent claims and 29 dependent claims). The following list summarizes the status of the claims:

1. Claims pending: 1-4, 6-27 and 29-34
2. Claims rejected: 1-4, 6-27 and 29-34
3. Claims allowed: none
4. Claims withdrawn from consideration: none
5. Claims canceled: 5 and 28

IV. STATUS OF AMENDMENTS (37 C.F.R. §41.37(c)(1)(iv))

This Response is the sole Response filed subsequent to the Final Office Action mailed on September 19, 2005. There are no unentered amendments.

V. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. §41.37(c)(1)(vi))

The grounds of rejection to be reviewed on appeal are:

A. The rejection of claims 1-4, 9-27, 29-32 under 35 U.S.C. §103 as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545); and

B. The rejection of claims 1, 15 and 21 under 35 U.S.C. §103 as purportedly being obvious over GB Patent Application 2,262,633 (Eustace) in view of IBM TDB "Data protection at the VOLUME level" (IBM).

VI. ARGUMENT (37 C.F.R. §41.37(c)(1)(vii))

A. The Combination of Ericson and Yu is Improper

The Final Office Action mailed September 19, 2005 rejects claims 1-4, 9-27 and 29-32 under 35 U.S.C. 103(a) as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545). Applicant respectfully traverses this rejection.

i. The Final Office Action Fails to Establish a Prima Facie Case of Obviousness

MPEP §2142 states, “[t]o establish a *prima facie* case of obviousness...there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.” The legal concept of *prima facie* obviousness allocates the initial burden of producing factual support to the Examiner (MPEP §2142). In particular, the Examiner bears the initial burden of establishing that there is some suggestion or motivation to combine the references.

The final Office Action has failed to produce evidence from the references or elsewhere to support the allegation that there is motivation to combine Ericson and Yu. In the “Response to Arguments” section, the final Office Action asserts that “both Ericson and Yu are directed to improving access security, hence they are analogous art.” During the telephone conference, the Examiner re-asserted this position, further alleging that since both Ericson and Yu involve access security in a network environment, it would have been obvious to use the authentication measures described in Yu to improve the access security of Ericson. However, even if it is true that Ericson and Yu are in the same field, that alone does not prove motivation to combine the references.

The Office Action must show incentive to combine the teachings of the two references. In *Ex parte Skinner* (Decision of the Board of Patent Appeals and Interferences, No. 650-69), the Board stated that “[w]hen the incentive to combine the teachings of the references is not readily apparent, it is the duty of the examiner to explain why the combining of the reference teachings is proper.” The final Office Action fails to provide any evidence that Yu’s authentication

methods actually *would* improve the security of Ericson. Not all networks are the same, nor do they exhibit the same security concerns. A security measure taken in one environment may be entirely irrelevant in another, and may not improve security, but rather may be an unnecessary design implementation. The Office Action's contention that the authentication methods of Yu would have somehow improved the security of the network storage system of Ericson is entirely unsupported, as the Office Action never shows (or even attempts to show) why this assertion would have been true.

To establish a *prima facie* case of obviousness, it must be shown *why* one skilled in the art, viewing the references at the time of the invention, would have been motivated to add Yu's authentication into Ericson (*Ex parte Skinner*). Accordingly, the Office Action has the burden of showing why one skilled in art would have believed that authentication would have improved security in the Ericson system. Merely stating that Yu's authentication would have improved the security of Ericson without factual support from the references is not sufficient to meet the Office Action's burden. Accordingly, the Office Action has not established a *prima facie* case of obviousness, and the rejection is therefore improper.

ii. There is No Motivation to Combine Ericson and Yu.

As discussed above, the Office Action has failed to meet the burden of showing motivation to combine Ericson and Yu. Therefore, Applicant need not produce evidence to the contrary (MPEP §2142). However, even though Applicant is not obligated to show why it would not have been obvious to combine Ericson and Yu, Applicant provides below support from the references showing that the authentication techniques of Yu would not in fact improve the security of Ericson, so that one skilled in the art would not have been motivated to modify Ericson as alleged in the Office Action because it would have merely complicated the system with unnecessary measures that do not improve security.

a. Discussion of Ericson

Ericson is directed to controlling access to a target device 102 (e.g., a disk array) by initiators 100 interconnected by a small computer system interface bus ("SCSI bus") 104, wherein the network devices are preconfigured in accordance with the SCSI specification. (Col.

3, lines 48-56). The initiators 100 request access to the target 102 by directing an access message to the target 102 via the SCSI bus 104, the message including the initiator identifier, a target identifier and a portion of the target device 102 to be accessed (i.e., the logical unit 108). (Col. 3, lines 56-61). Access to the target device is controlled by a look-up structure preconfigured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. When an initiator requests access, the look-up structure is indexed to check whether the initiator has been authorized to access the logical unit identified in the access message before allowing the initiator to access the logical unit (Col. 2, lines 26-65).

b. Discussion of Yu

Yu is directed to distributed security measures in an intelligent network having a plurality of interconnected network nodes, each having specified resources (e.g., a distributed telecommunication network architecture). The various nodes store objects associated with network resources having sets of interface operations describing the services provided by the respective object. Nodes can access the network resources of an object through the invocation of the service elements of the interface of the corresponding object. (Col. 5, lines 1-11). Objects can be identified and protected using a mechanism called a capability. A capability is a unique identifier of an object and a permission that gives a node the right to access the object. When a node requests a service provided by an object residing at another node (referred to as the execution node), a capability for the object is returned to the requesting node, giving it access to the services in the object permitted by the capability. (Col. 5, line 62 – Col. 6, line 11).

With the intelligent network architecture, outside service providers can access service elements of the telephone network. Yu teaches that in a distributed architecture, protection mechanisms for network security and integrity should themselves be distributed, but that if so they are vulnerable to forgery, theft, modification or destruction. (Col. 4, lines 37-65). Because an intruder in such a distributed network can forge almost all parts of a transmitted message except the node address (e.g., the network interface hardware or other low level control), Yu teaches that unique encryption keys be exchanged between an execution node and a node requesting a capability from the execution node, based on the low level hardware address (Col. 6

line 34 – col. 8 line 60). If a capability cannot be decrypted using the unique pairing of keys, the execution node knows that the capability has been tampered with, or an imposter node transmitted the capability of another node. (Col. 7 line 45 – col. 8 line 60).

c. Trusted and Untrusted Environments

From a security standpoint, the networks described in Ericson and Yu are very different and therefore exhibit different security concerns. In particular, as discussed below, Ericson describes a networked data storage system operating in a trusted environment. Yu describes a network for providing various services in an untrusted environment. A trusted network environment is one wherein devices seeking access to a resource are trusted not to spoof (or are incapable of spoofing) another's identity to hijack the access permissions allocated to another device. In such an environment, it is sufficient to allocate access privileges to each device that selectively allow and prevent devices from accessing portions of a resource according to the allocated access privileges, a process referred to as *authorization*.

In an untrusted network, the network may be widely distributed and the devices on the network may be unknown to the owner of the resource, making the network vulnerable to intruders or other bad actors (see e.g., Yu, cols. 8 and 9). Accordingly, authorization may not be sufficient because a request representing itself as being from a particular device cannot be trusted to have genuinely been sent from that device rather than from another device attempting to spoof its identity to gain unauthorized access to information. Accordingly, Yu implements authentication techniques to verify that a device is actually the device it represents itself to be, thus preventing unauthorized access to a resource via spoofing or capability theft.

It should be appreciated from the foregoing that *authorization* and *authentication* are two distinct security measures that address separate and distinct security issues. Authentication techniques are unnecessary in a trusted environment and do not serve to increase security, but rather add unnecessary complexity to the access management scheme in a trusted environment.

Nowhere does Ericson discuss untrusted environments or any type of security breaches requiring authentication. Furthermore, not only is Ericson silent about an untrusted environment, but Ericson provides evidence that the authentication system disclosed is for use in a trusted

environment. In particular, the controlled data storage access system of Ericson is performed in a SCSI environment where initiators are trusted. As discussed below, both the nature of the SCSI environment and the details of the SCSI interface make it unnecessary and therefore undesirable to implement verification or authentication methods as disclosed by Yu.

The SCSI protocol defines a standard for communication between a computer and various peripheral devices. In particular, various host devices (referred to as initiators) may issue requests to one or more peripheral devices (referred to as targets) that are connected to the SCSI bus. Each device (i.e., an initiator or a target) has a unique SCSI ID which identifies its physical location on the SCSI bus. The narrow SCSI bus and associated connectors support a maximum of eight devices. The wide SCSI bus and associated connectors support a maximum of 16 devices. See e.g., <http://www.infran.ru/TechInfo/BSD/handbook114.html>; <http://scsifaq.paralan.com/>.

The SCSI environment is local and contained, and therefore trusted and secure. Only a limited number of devices can be attached to a SCSI bus over a limited and local area. For example, internal SCSI connections (i.e., SCSI ribbon connections) are designed for communication between components and peripherals within the same computer (e.g., a personal computer). See e.g., <http://computer.howstuffworks.com/scsi5.htm>. External SCSI connections (i.e., SCSI cables) are designed to connect peripherals over relatively short distances. For example, SCSI cables typically come in 3ft and 6ft lengths. Although the cables may be daisy-chained, the SCSI protocol itself does not support bus lengths greater than 25 meters. Accordingly, a SCSI network is limited to a small area and limited to a small number of devices. See e.g., http://www.ramelectronics.net/html/scsi_connectors.html#cablelength.

In addition, each device on the SCSI bus must be manually configured and physically connected to the bus via an appropriate SCSI connector, and assigned a unique SCSI ID (often by manually setting a physical switch or configuring external jumpers). To assign a unique SCSI ID to a device (i.e., 0-7 for narrow SCSI and 0-15 for wide SCSI), the SCSI ID of every other device on the bus must be known to avoid conflicts. See e.g., <http://computer.howstuffworks.com/scsi3.htm>;

http://www.seagate.com/support/kb/tape/w4m_scsi.html;

<http://support.gateway.com/s/CDROM/Panasonic/CS006aa/PANAS100.shtml>.

Accordingly, there are no unknown or untrusted devices connected to a SCSI bus. An operator or administrator building a SCSI network must physically attach each device to the bus and configure it appropriately. <http://www.sun.com/solutions/blueprints/0800/scsi.pdf> (see especially “SCSI Issues in Clusters” on page 3, *et. seq.*) Therefore, the operator is cognizant of each device on the network and is fully in control of what devices are connected to the SCSI bus. That is, untrusted devices cannot gain access to the SCSI bus. In such a local and trusted environment, it would have been unnecessary to implement verification and/or authentication procedures.

Furthermore, the SCSI interface itself prevents a device from misrepresenting its identity. The SCSI ID assigned to each device connected to a SCSI bus both identifies the device and specifies the device’s physical address on the bus. The uniqueness of a SCSI ID is a requirement of the interface. <http://www.sun.com/solutions/blueprints/0800/scsi.pdf>. For example, bus arbitration and communication depends on each attached device having a unique SCSI ID. Conflicts with SCSI IDs prevent the conflicting devices from gaining access and communicating over the SCSI bus (and may result in the failure of all devices on the SCSI bus). <http://www.ba-stuttgart.de/~schulte/htme/ebuss12.htm#REF2.1.2>. The uniqueness of a device’s SCSI ID is its license to access the bus. For a device to communicate over the bus, it must represent itself by that unique SCSI ID. Accordingly, there is no way for a device to misrepresent itself without disrupting the SCSI network. <http://www.infran.ru/TechInfo/BSD/handbook115.html#210>.

In Ericson, a plurality of initiators 100 are connected via a SCSI bus 104 to a target device 102 such as a disk array having a controller 106 (col. 3, line 53 – col. 4, line 5). Upon request by an initiator, the controller accesses a look-up data structure that defines which initiators have access to which logical units of the disk array to ensure that the request is permitted (col. 4, lines 6-54). In Ericson, the allocation of logical units to particular initiators is conducted in a trusted environment. For example, column 4, lines 54-61 state:

The look-up data structure may be pre-configured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. This preconfiguration preferably is performed when the target controller 106 is installed. When necessary, however, the look-up data structure may be reconfigured at any subsequent time, such as when new initiators 100 are added to the system, or when the logical units 108 must be reassigned to other initiators 100.

The system operator is in complete control of the local SCSI network. The system operator configures the look-up data structure according to the devices on the SCSI bus and allocates logical units to new devices added onto the SCSI bus as desired. The system operator is trusted with properly adding devices to the SCSI bus and defining the look-up data structure to permit access as desired by associating initiator IDs with desired logical units. In a SCSI environment, the system operator must give each device a unique SCSI ID which must remain unique in order for a device to communicate on the bus.

In this environment, there is no opportunity for a device to misrepresent its identity to gain access to restricted logical units of the target device. The SCSI network is a local and contained network of devices wherein the administrator of the network has control over connecting each of the devices, configuring their SCSI ID's and allocating their respective permissions. Not only are there no untrusted devices on the SCSI network, but the SCSI network itself prevents devices from spoofing their identity to gain access credentials of another device.

While Ericson mentions that other peripheral interfaces may be used, Ericson does not contemplate untrusted environments or anywhere suggest that the described access method could be used in environments where there is a possibility that initiators may attempt to misrepresent their identity to gain access to restricted logical units. In particular, nowhere does Ericson disclose an environment where untrusted devices have access to the data storage, nor does Ericson suggest that spoofing is, or would be, a problem. Accordingly, authenticating the identity of a device is completely unnecessary in Ericson.

iii. Summary of Arguments Regarding Ericson and Yu

In the "Response to Arguments" section, the final Office Action asserts on page 2 that the motivation to combine Ericson and Yu is that Ericson benefits from "the advantage of [Yu's]

security method.” As discussed above, the Office Action has the burden of showing that authentication is in fact an advantage in Ericson. In order for the Office Action’s assertion to operate as valid motivation to combine Ericson and Yu, the Office Action must demonstrate that there is a threat in Ericson that would justify adding authentication security measures. Absent a security threat that would be remedied by authentication, one of ordinary skill in the art simply would not have been motivated to add unnecessary complexity and expense. Analogously, no one would be motivated to purchase snow tires for their car in Southern California. It is senseless to protect against non-existent threats.

Applicant has produced evidence that there is in fact no security threat in Ericson that would be remedied by Yu’s authentication. However, it is not Applicant’s burden to conclusively establish the absence of a threat in Ericson that could be remedied by authentication, as it is the Office Action’s burden to prove that such a threat exists in Ericson. The Office Action has failed to produce any such evidence, and therefore has failed to establish a *prima facie* case of obviousness. Accordingly, Applicant respectfully requests that the rejection be withdrawn.

B. The Claims Patentably Distinguish over Eustace in view of IBM

The Office Action also rejects claims 1, 15 and 21 under 35 U.S.C. 103(a) as purportedly being obvious over GB Patent Application 2,262,633 (Eustace) in view of IBM TDB “Data protection at the VOLUME level” (IBM). Applicant respectfully traverses this rejection. Applicant does not concede that there is motivation to combine the two references. However, even if there would have been motivation to modify Eustace based on IBM as alleged in the Office Action, the combination does not disclose each of the limitations of the rejected claims. Applicant reserves the right to argue against the combination in the future if so desired.

i. The Alleged Combination Does Not Show All the Limitations of the Claims

The Office Action asserts that Eustace discloses a step of verifying that the represented source of the request is the device that issued the request. Applicant respectfully disagrees. The Office Action cites page 5, lines 3-6 in Eustace as allegedly disclosing this step. The cited excerpt reads, “[t]he monitoring circuit is also constructed to identify the source processor of an

address instruction and to identify from the address instruction the file to which access is sought.” However, this does not describe an act of verifying the identity of the processor but rather merely reports taking the represented identity along with the target file address to index an authorization table.

In particular, Eustace describes a security apparatus in which a processor seeking to access a file in a storage system is checked against cross-reference table 8 to check if the table includes an authorized status indicator of 1 (authorized) or 0 (not authorized) for the file which the processor is attempting to access. (page 4, lines 9-19). This is authorization, not authentication or verification. The monitoring circuit is merely taking the represented identity sent by the processor and the file address at which access is being sought. The processor and file address are then used to index into cross-reference table 8 to determine whether the processor is authorized to access the file. Eustace is completely silent with respect to authentication, verification or problems associated with a processor spoofing its identity. Eustace merely authorizes a processor to access a file, but nowhere discloses or suggests verifying that the processor is actually who it represents itself to be. The IBM reference does not cure this deficiency.

Claim 1 recites a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, the method comprising steps of receiving over the network at the storage system a request from one of the at least two devices for access to at least one of the plurality of volumes of the storage system. The request identifies the at least one of the plurality of volumes in the storage system and a represented source of the request. Managing access to the storage system includes selectively servicing the request, at the storage system, based at least in part on steps of determining, from configuration data, whether the represented source is authorized to access the at least one of the plurality of volumes, and *verifying that the represented source of the request is the one of the at least two devices that issued the request.* (Emphasis added).

Nowhere does the combination of Eustace and IBM disclose or suggest “verifying that the represented source of the request is the one of the at least two devices that issued the

request,” as recited in claim 1. Therefore, claim 1 patentably distinguishes over the combination and is allowable condition.

Claim 15 recites a computer readable medium comprising a first data structure to manage accesses by a plurality of devices to volumes of data at a storage system over a communication network, the storage system managing access responsive to requests that each identifies one of the plurality of volumes of the storage system to be accessed and one of the plurality of devices that is represented as having issued the request. The first data structure comprises a plurality of records corresponding to the plurality of devices, the plurality of records comprising at least one record corresponding to one of the plurality of devices and including configuration information having at least one identifier that identifies which of the volumes of the storage system the one of the plurality of devices is authorized to access. The at least one record also includes *authentication information that can be used by the storage system to determine whether the one of the plurality of devices that issued the request is the corresponding one of the plurality of devices.* (Emphasis added).

Nowhere does the combination of Eustace and IBM disclose or suggest a computer readable medium including a first data structure having at least one record including configuration information having “authentication information that can be used by the storage system to determine whether the one of the plurality of devices that issued the request is the corresponding one of the plurality of devices,” as recited in claim 15. Therefore, claim 15 patentably distinguishes over the combination and is allowable condition.

Claim 21 recites a storage system comprising at least one storage device apportioned into a plurality of volumes, a configuration table to store configuration data identifying which of a plurality of devices coupled to the storage system via a network are authorized to access which of the plurality of volumes, and a filter, responsive to the configuration data, to selectively forward to the at least one storage device requests for access to the plurality of volumes received from the plurality of devices over the network. Each request identifies at least one of the plurality of devices that is represented to the storage system as having issued the request. *The*

filter is adapted to verify that the at least one of the plurality of devices identified in the request is the device that issued the request. (Emphasis added).

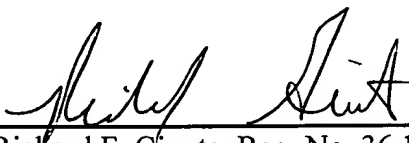
Nowhere does the combination of Eustace and IBM disclose or suggest a storage system including a filter responsive to configuration data and adapted to "verify that the at least one of the plurality of devices identified in the request is the device that issued the request," as recited in claim 21. Therefore, claim 21 patentably distinguishes over the combination and is allowable condition.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,
Steven M. Blumenau et al., Applicant

By: 
Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No.E0295.70066US00
Date: December 19, 2005
x12/19/05